



Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Privacy-Enhanced Event Scheduling

<http://dudle.inf.tu-dresden.de>

Sandra Steinbrecher

Frankfurt, Germany, March 29, 2010



Event Scheduling



Event Scheduling

Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 2 of 6

- Meeting, TelCo
- MS exchange, Outlook, Thunderbird, doodle
- common in all solutions: publish availability pattern
- next: define "Privacy-Enhanced Event Scheduling"
- 2 different privacy problems occur

Privacy Problems

Direct Inference

Doodle Poll: Business Dinner

	Mon 19	Tue 20	Wed 21	Thu 22
John	yes	yes	yes	yes
Peter	yes	yes	yes	yes
Julie	yes	yes	yes	yes
Tom	yes	yes	yes	yes

My husband wants the date of our wedding, no way!

Problem Statement

Event Scheduling

Direct Inference

Indirect Inference

Solution

Solution?

Register

Privacy Problems

Direct Inference

Will my husband vote for the date of our wedding anniversary?

Doodle®

Poll: Business Dinner

October 2009					
	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
	8:00 PM	8:00 PM	8:00 PM	8:00 PM	8:00 PM
John	OK		OK	OK	OK
Peter		OK		OK	OK
Julie	OK	OK		OK	
Tom		OK	OK	OK	OK
Your name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count	2	3	2	4	3

Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 3 of 6

- business dinner
- john's wife asks herself

TECHNISCHE
UNIVERSITÄT
DRESDEN

Privacy Problems

Direct Inference

Doodle® Poll: Business Dinner

	Mon 19	Tue 20	Wed 21	Thu 22	Fri 23
John	OK		OK	OK	OK
Peter		OK		OK	OK
Julie	OK	OK		OK	
Tom		OK	OK	OK	OK
Your name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count	2	3	2	4	3

Will my husband vote for the date of our wedding anniversary?

Count: 2 3 2 4 3

Privacy-Enhanced Event Scheduling

Slide 3 of 6

Problem Statement

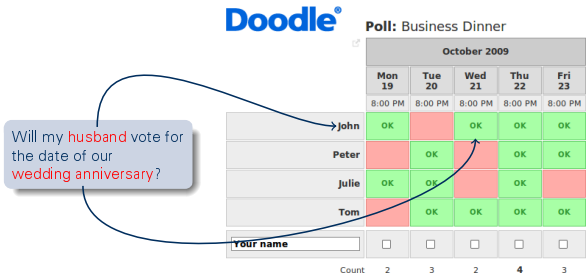
Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Privacy Problems

Direct Inference



Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 3 of 6

- business dinner
- john's wife asks herself

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

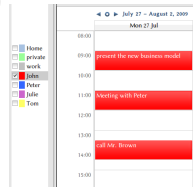
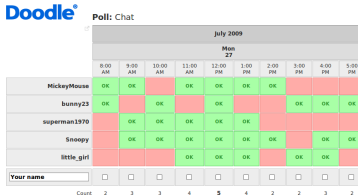
Solution

Solution?
Register

Privacy Problems

Indirect Inference

The availability pattern of user bunny23 looks suspiciously like the one of my employee John Doe!

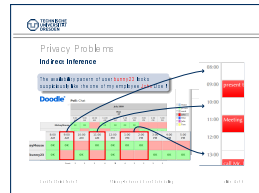


Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 4 of 6

- matching 2 information sources
- identify pseudonyms
- it is not enough to use doodle pseudonymously



Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

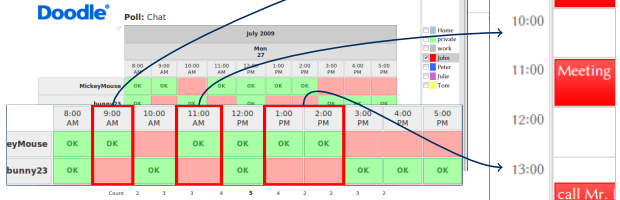
Solution

Solution?
Register

Privacy Problems

Indirect Inference

The availability pattern of user **bunny23** looks suspiciously like the one of my employee **John Doe**!

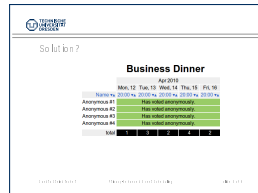


Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 4 of 6

- matching 2 information sources
- identify pseudonyms
- it is not enough to use doodle pseudonymously



Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Solution?

Business Dinner

Apr 2010					
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Anonymous #1	Has voted anonymously.				
Anonymous #2	Has voted anonymously.				
Anonymous #3	Has voted anonymously.				
Anonymous #4	Has voted anonymously.				
total	1	3	2	4	2

Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 5 of 6

- naive solution, schedule-decision on sum of availabilities
- Without identification of participants, attackers stay anonymous

Solution?

Business Dinner

Apr 2010

	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carl	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2

Slide 5 of 6

Privacy-Enhanced Event Scheduling

Slide 5 of 6

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Solution?

Business Dinner

Apr 2010					
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2

Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 5 of 6

- naive solution, schedule-decision on sum of availabilities




So l u t i o n ?

Business Dinner

Apr 2010

	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2



Copyright © 2010 Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

Slide 5 of 6

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Solution?

Business Dinner

Apr 2010					
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2



Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 5 of 6

- naive solution, schedule-decision on sum of availabilities
- in this naive approach, trust in server is needed

TECHNISCHE
UNIVERSITÄT
DRESDEN

Solution?

Business Dinner

Apr 2010

	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2

Server

Confidential Solution? Privacy-Enhanced Event Scheduling Slide 5 of 6

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Solution?

Business Dinner

Apr 2010					
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2



Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 5 of 6

- naive solution, schedule-decision on sum of availabilities
- Untrusted Server

So l u t i o n ?

Business Dinner

Apr 2010

	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2

So l u t i o n ?

Privacy-Enhanced Event Scheduling

slide 5 of 6

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Solution?

Business Dinner

	Apr 2010				
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2



Sandra Steinbrecher



Privacy-Enhanced Event Scheduling

slide 5 of 6

- naive solution, schedule-decision on sum of availabilities
- Untrusted Server
- Cryptographic Methods to overcome servertrust

So l u t i o n ?

Business Dinner

	Apr 2010				
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲	20:00 ▼▲
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2

Untrusted Server

Privacy-Enhanced Event Scheduling

Slide 5 of 6

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Solution?

Business Dinner

	Apr 2010				
	Mon, 12	Tue, 13	Wed, 14	Thu, 15	Fri, 16
Name ▼	20:00 ▼	20:00 ▼	20:00 ▼	20:00 ▼	20:00 ▼
Bob	Has voted anonymously.				
Carol	Has voted anonymously.				
Alice	Has voted anonymously.				
Dave	Has voted anonymously.				
total	1	3	2	4	2



Sandra Steinbrecher



Privacy-Enhanced Event Scheduling

slide 5 of 6

- naive solution, schedule-decision on sum of availabilities
- Untrusted Server
- Cryptographic Methods to overcome servertrust
- key ids behind names

Register

SecretKey:

Copyright 2010 Sandra Steinbrecher, Technische Universität Dresden. All rights reserved.

Problem Statement

Event Scheduling
Direct Inference
Indirect Inference

Solution

Solution?
Register

Register

Secret Key:

1848baf5fbc94ac77119e2ea58af58f5c23cadfa5a08639516dcc82315fa6bad046cda38893fbf703d42c5152f587fcc14b721
3e7650504022160b7dff37235039951f0098b04b92957bf6b060477dbf3fee4a17bbb4385878098c2bff6f06831df4c

Cancel


Login

Sandra Steinbrecher

Privacy-Enhanced Event Scheduling

slide 6 of 6

- registration phase is needed to exchange asymmetric keys



TECHNISCHE
UNIVERSITÄT
DRESDEN

www.tu-dresden.de

Thank you for your attention!

<http://dalle.inf.tu-dresden.de>

Sandra Steinbrecher

Frankfurt, Germany, March 29, 2010



Thank you for your attention!

<http://dudle.inf.tu-dresden.de>

Sandra Steinbrecher

Frankfurt, Germany, March 29, 2010

This is the last
slide!